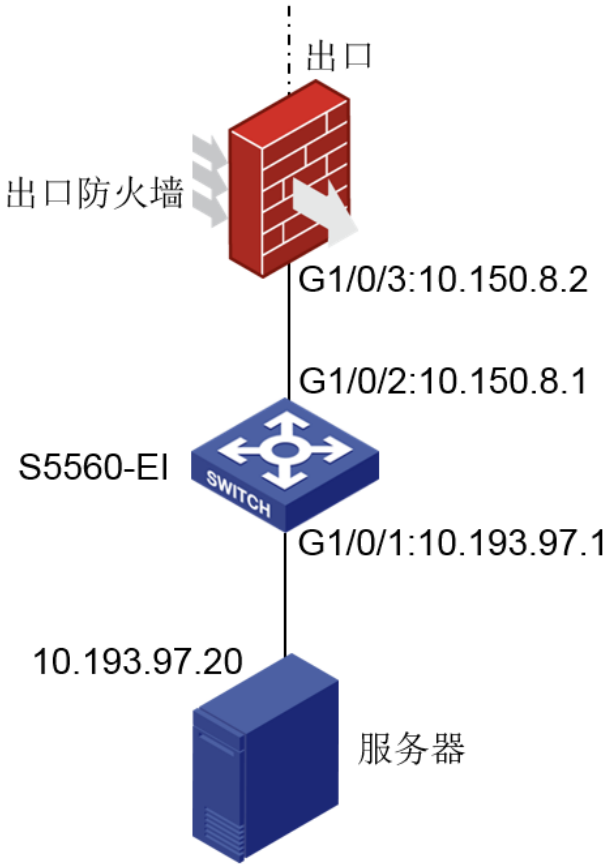
某局点V7防火墙F1030无法ping通内网服务器问题排查

NAT 静态路由 徐猛 2019-06-02 发表

组网及说明

现场组网大致拓扑如下，防火墙F1030作为内网服务器以及终端的出口设备，服务器的网关在S5560-EI交换机上。现场服务器有访问互联网的需求。



问题描述

现场使用内网服务器访问外网不通，然后首先进行分段测试，发现服务器无法正常ping通防火墙，从防火墙也无法ping通服务器。具体ping测试情况如下。

[F1030]ping -a 10.105.8.2 10.193.97.1
Ping 10.193.97.1 (10.193.97.1) from 10.105.8.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

过程分析

1.对于防火墙到服务器不通这种问题，我们首先的思路是，检查下防火墙的安全策略是否正确放通，以及两边设备的路由是否正常。

（1）首先检查防火墙的安全策略配置：

```
security-zone name Trust
 import interface GigabitEthernet1/0/3        //内网接口
#
security-policy ip
 rule 1 name GuideSecPolicy
  action pass
  source-zone Local
  source-zone Trust
  source-zone Untrust
```

source-zone DMZ
destination-zone Untrust
destination-zone DMZ
destination-zone Trust
destination-zone Local

经检查安全策略，local安全域到内网口3口所在的trust安全域是全放通的，另外在防火墙上ping内网直连地址10.150.8.1是正常通的。

（2）其次我们对设备上的路由配置以及服务器网关进行了检查：

ip route-static 0.0.0.0 0 192.168.250.57 //指向出口下一跳的缺省路由
ip route-static 10.193.97.0 24 10.105.8.1

发现设备上出了指向出口下一跳的缺省路由外，就只有去往服务器的一条明细路由了，防火墙路由配置没有问题。

（3）后续检查了下服务器网卡网关配置正确，网关地址为交换机的10.193.97.1地址，并且从服务器上ping交换机的10.150.8.1地址是通的。说明服务器路由正常，报文转发正常。

（4）为了确认下该异常情况是否由防火墙导致，我们在防火墙上进行了ping -a 10.105.8.2 10.193.97.20操作，然后查看对应的会话，情况如下：

[F1030]display session table ipv4 source-ip 10.105.8.2 destination-ip 10.193.97.20 verbose
Slot 1:
Total sessions found: 0

由此测试结果，可以确认问题出现在了防火墙上，由于没有相应会话，那么只有两种可能原因，一种是安全域未放通，另一种是路由转发存在问题。但是对于第一种安全域未放通这个原因，首先可以排除，因为安全策略是全放通的，而且内网接口下联的交换机是能通的。

（5）针对（4）中排查的情况，怀疑是否是路由下发异常导致的，于是查看了路由表：

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.193.97.0/24	Static	60	0	10.105.8.1	GE1/0/3
10.193.97.1/32	Direct	1	0	0.0.0.0	NULL0
10.193.97.2/32	Direct	1	0	0.0.0.0	NULL0
10.193.97.3/32	Direct	1	0	0.0.0.0	NULL0
10.193.97.4/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.8/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.12/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.16/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.32/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.48/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.64/26	Direct	1	0	0.0.0.0	NULL0
10.193.97.128/26	Direct	1	0	0.0.0.0	NULL0
10.193.97.192/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.208/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.224/28	Direct	1	0	0.0.0.0	NULL0
10.193.97.240/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.244/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.248/30	Direct	1	0	0.0.0.0	NULL0
10.193.97.252/32	Direct	1	0	0.0.0.0	NULL0
10.193.97.253/32	Direct	1	0	0.0.0.0	NULL0
10.193.97.254/32	Direct	1	0	0.0.0.0	NULL0

发现在防火墙上，10.193.97.0/24网段的地址，几乎都存在掩码高于24位的，下一跳指向NULL0的路由条目，而导致24位掩码长度的正常路由优先级低，在转发报文的时候，未被启用。但是由于下一跳指向NULL0的路由条目在设备上会被直接丢弃，所以去往该目的网段的报文会被丢弃而无法正常转发。

（6）针对（5）中分析出的情况，又有了疑问，设备上为什么会出现下一跳指向NULL0的路由呢，后来我们仔细检查了下设备的完整配置，发现了如下的配置内容：

nat address-group 1 name server
address 10.193.97.1 10.193.97.254

现场实施工程师在设备上配置了个nat outbound转换用的地址组，该地址组中包含了内网服务器所在的网段。根据设备的报文转发原理，我们在设备添加nat outbound相关配置的时候，设备会自动将nat转换后的地址在设备上生成一条对应的NULL0路由，来保证报文能在设备上进行终结。也正是由于现场做的这个错误配置，导致设备上会生成内网服务器网段的NULL0路由，也导致现场出现的转发异常的情况。

解决方法

现场错误的配置是由于现场工程师对nat outbound地址转换机制不了解导致的，和现场实施工程师说明相关nat outbound地址转换机制和原理后，修改nat address-group地址组中的地址为其他网段，并保证外网回程路由，能正确将去往该地址组网段的报文转发到防火墙上即可。